TREATMENT, PROTECTION, AND CONFIDENTIALITY OF PERSONAL DATA WHEN TRANSLATING CLINICAL TRIALS

Within Telelingua's Life Sciences Department, through the nature of the files we translate, we may be confronted with sensitive data or confidential information (confidential study results and statistics, possibly personal information).

Personal data could be:

- Names
- Addresses
- Dates of birth
- National insurance numbers
- Any information that would enable the identification of the person concerned.

Treatment of confidential data

It is our customer's responsibility to protect personal data and information, and to ensure that it is properly redacted (anonymized or semi-anonymized[1]) before the files are sent to us for translation. Since anonymization is thus normally done in the source files *before* delivery to Telelingua, our employees have no access to this data, and cannot carry out any actions with them.

However, should Telelingua receive a file still containing personal data (e.g. a hospital discharge summary in which the patient's details have not been redacted), Telelingua will immediately inform the customer hereof, asking him to anonymize the data and send us a new file.

However, if the customer is not able to anonymize this information, the project manager at Telelingua must then take the necessary measures to ensure that the personal information is no longer visible in the source file. This is done with a tool that allows us to modify PDF documents. Once all the personal data is deleted, we make sure to overwrite the previous electronic version.

Access to confidential data

To ensure the security of all the records held by Telelingua, it is necessary to have structured user permissions to control which users or groups require access to which areas of the file management systems, the ERP, software and their own computer. User permissions are defined and set by the IT department in consultation with department leads. Permissions are

[1] Semi-anonymization means that the personal data (e.g., names) are replaced by reference numbers.

set by role/job titles, so that only the Accounting Department, for example, can access the accounts, whereas a project manager has access to project-related areas in the ERP.

In order to control the software used by the team, only the IT Department is authorized to install applications, after they have been tested and found to perform the required functions within the defined environment.

Security and protection of data and files

Should the customer leave Telelingua, our Life Sciences Department Coordinator will delete the customer's account after a period of prolonged inactivity. The IT Department generates a log of inactive accounts to be validated by the Life Sciences Department Coordinator before proceeding with the deletions. The customer can be provided with a report of deleted files, upon request.

All electronic documents are exchanged via secured media (encrypted mail, secured FTP or secured portal). The IT system is a closed-loop circuit (not accessible from outside the firewall), and no external parties are involved in tasks such as back-up. All finalized projects are stored on an archive volume and removed from the active volume (SAN). The archives are kept on-line but can only be read. The archived projects are archived on the NAS and also copied onto tapes (stored in a fire-retardant safe). All data is replicated in another Telelingua office. Back-up and replication procedures are documented in an SOP.

Telelingua has a powerful antivirus system installed on our servers and on each computer. We have two firewalls (front-end and before SAN), and anti-spam filtering on the firewall (front-end and Internet). We also follow SOPs for passwords on confidential documents and on our portals (password expiration policy with automatic password aging feature and Portal Certification and Security (DSR)).

Telelingua uses the *Veeam Backup & Replication* system. The back-ups are encrypted and have three security levels:
- First level: daily local internal back-up of all network servers
- Second level: weekly local back-up on a tape device system
- Third level: daily replication of all network servers between the Telelingua entities

In other words, the data is backed up locally on separate servers/supports and are also backed up in remote Telelingua entities. This means that the data is backed up several times and in several locations.

Confidentiality by freelance translators involved in the translation project

Telelingua also ensures confidentiality when and to the extent that it calls on freelance translators in the context of a translation project. Telelingua's translators are conscious of the confidential nature of sensitive data, and are reminded that such information should not be visible in the source files. Should a translator receive files that contain personal data, this breach of data protection must be immediately escalated to Telelingua's department lead, who has a duty to notify the concerned parties, and help ensure that the necessary corrective actions are promptly taken.

All our translators sign a very strict NDA (Non-Disclosure Agreement) which states, among others, that the translator is allowed to store *collateral material*[2] on a local data-bearing medium only for the duration of the project and a period of 1 month after the delivery. All and any collateral material must be returned to Telelingua upon first request or within 1 month at the latest after completion of the project.

In the event that collateral material cannot be returned, it must be destroyed or deleted within 1 month at the latest after completion of the project. It is forbidden for translators to keep copies of the collateral material in the Cloud or on any other data-bearing media in whatever format after the completion of the project; it is also forbidden to copy, reproduce or distribute any collateral material without prior express written approval from Telelingua. The translator is responsible for ensuring that neither collateral material nor any other information provided by Telelingua, in whatever format, is brought to the knowledge of third parties, without prior written authorization from Telelingua.

All members of the project management teams, the Quality Department, and the IT Department at Telelingua play a key role in treating and protecting possible personal data in the content that we translate. This brings an important added value to our customer service.

For more detailed information, contact our Data Protection Officer at dataprotection@telelingua.com

[2] Collateral material: including, but not limited to: translation source and target files, translation memories, terminology databases, etc.